

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**

02/12/2012

**SUBJECT:**

Adobe Shockwave Player Remote Code Execution Vulnerability

**OVERVIEW:**

A vulnerability has been discovered in Adobe Shockwave Player which could allow for remote code execution. Adobe Shockwave Player is a multimedia platform used to add animation and interactivity to web pages. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**SYSTEMS AFFECTED:**

- Adobe Shockwave Player 11.6.8.638 and earlier versions for Windows and Macintosh

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**DESCRIPTION:**

Adobe Shockwave Player is prone to a remote code-execution vulnerability because of a memory corruption vulnerability and a stack overflow vulnerability. Attackers can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will likely result in denial-of-service conditions. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**

The following actions should be taken:

- Update Adobe Shockwave Player on vulnerable systems immediately after testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

#### **REFERENCES:**

##### **Adobe:**

<https://www.adobe.com/support/security/bulletins/apsb13-06.html>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0635>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0636>